How to Configure the SSL VPN Service

https://campus.barracuda.com/doc/73719130/

The SSL VPN service is part of the VPN service on the CloudGen Firewall. Configure a listener for the SSL VPN on a public IP address and authenticate the users via a local or external authentication scheme. It is recommended to use signed SSL certificates to avoid SSL error messages when users access the SSL VPN portal. SSL VPN is supported for CloudGen Firewall F18 and larger, as well as all CloudGen Firewall Vx models except VF10.

Before You Begin

- An Advanced Remote Access subscription is required.
- Verify that the IP address you want the SSL VPN to listen on is configured as a virtual server and VPN service IP address. For more information, see Virtual Servers and Services.
- Configure an external authentication server or NGF local authentication. For more information, see Authentication.

Step 1. Disable Port 443 for Site-to-Site and Client-to-Site VPN

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN > VPN Settings**.
2. Click **Lock**.
3. Click **Click here for Server Settings** link. The **Server Settings** window opens.
4. Set **Port 443 VPN Listener** to **No**.

Server Configuration

Port 443 VPN Listener	No
CRL Poll Time (min)	0
Global TOS Copy	Off
Global Replay Window Size, Packets(0...Use Default)	

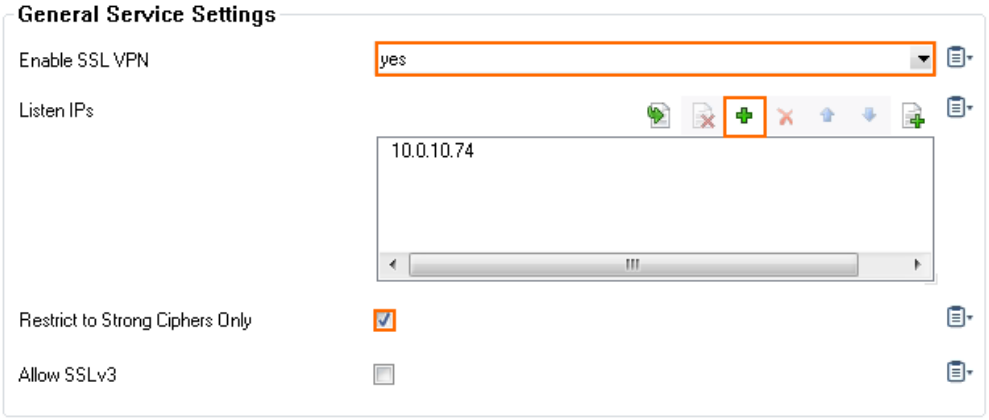
5. Click **OK**.
6. Click **Send Changes** and **Activate**.

Step 2. Configure SSL VPN General Service Settings

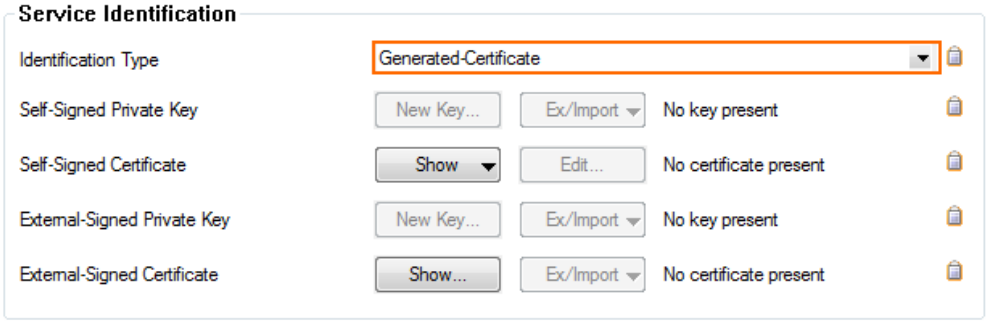
Enable the SSL VPN service and add the listening IP addresses.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > SSL-VPN**.
2. Click **Lock**.

3. Set **Enable SSL VPN** to **Yes**.
4. Click **+** to add a **Listen IP**.



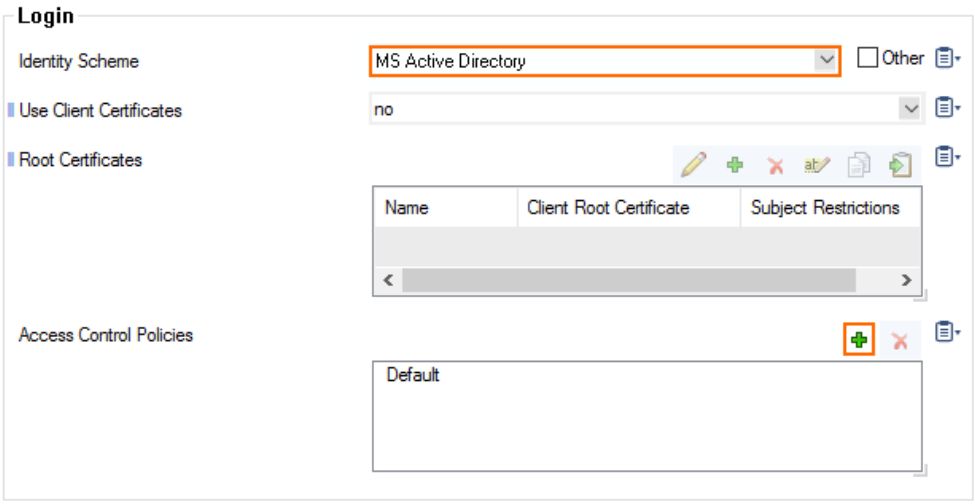
5. (recommended) Enable **Restrict to Strong Ciphers Only**.
6. Select the **Identification Type**:
   - **Generated-Certificate** – The certificate and the private key is automatically created by the firewall.
   - **Self-Signed-Certificate** – Click **New** to create a **Self-Signed Private Key** and then **Edit** to create the **Self-Signed Certificate**.
   - **External-Certificate** – Click **Ex/Import** to import the CA-signed **External Certificate** and the **External-Signed Private Key**.



7. Click **Send Changes** and **Activate**.

Step 3. Configure Login

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > SSL-VPN**.
2. In the left menu, click **Login**.
3. Click **Lock**.
4. In the **Login** section, set the **Identity Scheme** to your preferred authentication method, e.g., **MS-Active Directory**.
5. If a client certificate should be required,
   1. Set **Use Client Certificates** to **yes**. (This requires a restart of the VPN server.)
   2. Click **+** to add the **Root Certificates** used to verify peer certificates.
6. Click **+** to add your access control policy to the list of **Access Control Policies**.

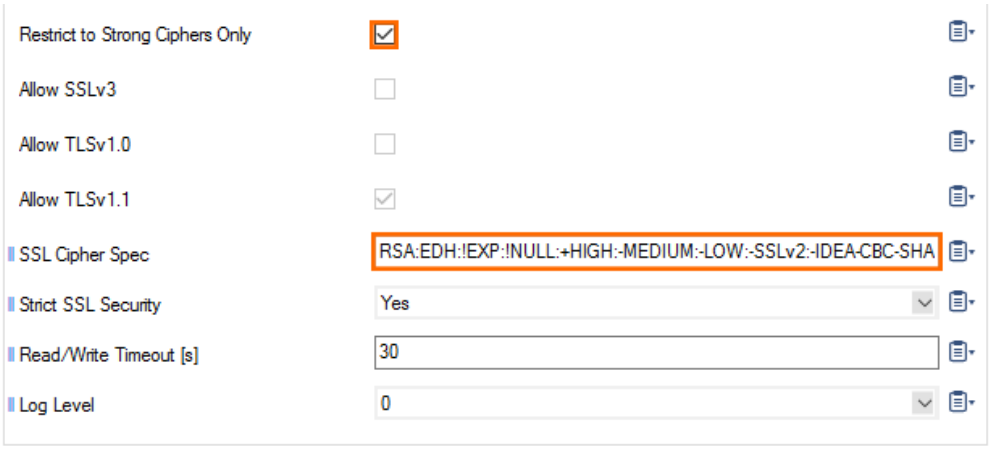


7. (optional) Configure the following settings as needed:
   - **Use Max Concurrent Users** – Enable to limit the number of simultaneous users using the SSL VPN service.
   - **Max Concurrent Users** – Enter the maximum number of users that can be simultaneously connected to the SSL VPN service.
   - **Session Timeout (m)** – Enter the session timeout in minutes.
   - **Deny Remember Me** – Set to **yes** to remove the **Remember me** check box on the login page.
8. Customize the login messages and logos:
   - (optional) Import a 200 x 66-pixel PNG or JPG image to customize the **Logo**.
   - (optional) Enter a plain text **Login Message**. E.g, `Welcome to the Barracuda CloudGen Firewall SSL VPN`.
   - (optional) Enter a HTML **Help Text**.
9. Click **Send Changes** and **Activate**.

Step 4. (optional) Use Custom Cipher String

Configure a custom cipher string to be used by the SSL VPN service.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > SSL-VPN**.
2. In the left menu, click **Basic Setup**.
3. Click **Lock**.
4. In the left menu, expand **Configuration Mode** and click on **Switch to Advanced View**.
5. Disable **Allow SSLv3**.
6. Enable **Restrict to Strong Ciphers Only**.
7. Enter your custom **SSL Cipher Spec** string.



8. Set **Strict SSL Security** to **yes**.
   This setting might break access for some older client SSL implementation. Disable if you experience problems when using older browsers.
9. Click **Send Changes** and **Activate**.

Troubleshooting

- If the **sslvpn** log contains the following line: `http_listener: failed to listen on @443` verify that no other service on the firewall is running on that port and that no DNAT access rules are forwarding TCP port 443 (HTTPS) traffic.
- Restart the SSL VPN service after updating or changing certificates:
  1. Set **Enable SSL VPN** to **no**.
  2. Click **Send Changes** and **Activate**.
  3. Set **Enable SSL VPN** to **yes**.
  4. Click **Send Changes** and **Activate**.

Figures

1. disable_s2s_443.png
2. sslvpn01.png
3. sslvpn02.png
4. add_access_control_polic_00.png
5. strong_ciphers_00.png